Strategy Research Project

Assessment of U.S. Cybersecurity Management

by

Colonel Kelly T. Knitter
United States Army

United States Army War College
Class of 2012

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
22-03-2012	Strategy Research Project	

4. TITLE AND SUBTITLE
Assessment of U.S. Cybersecurity Management

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Colonel Kelly T. Knitter

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Professor Brian Gouker
Department of Military Strategy,
Planning, & Operations

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution: A

13. SUPPLEMENTARY NOTES

14. ABSTRACT

In early 2009, President Obama declared cyber threat as one of the most serious economic and national security challenges of the 21st century. In May 2009, he directed the U.S. Government Accountability Office (GAO) to review national level cybersecurity policies and procedures. Findings indicated two critical shortfalls: lack of leadership and lack of clearly defined roles among federal agencies. Although a new Special Assistant to the President and Cybersecurity Coordinator was appointed within the White House three years ago to lead federal agencies in cyber collaboration and synchronization, the overall assessment given by GAO indicates cybersecurity management at the national level needs much improvement. The purpose of this paper is threefold: (1) to identify the different roles, responsibilities, and authorities of cybersecurity management within the U.S. Government; (2) to assess the national level cybersecurity management program for efficiencies and effectiveness; and (3) to provide strategic options on ways to improve overall cybersecurity management which leads to effective protection and operations of U.S. networks and information in a resource constrained environment.

15. SUBJECT TERMS
Cyber, Network Security, Information Technology, Information Sharing, Cyber Strategy, Cyber Stakeholders, Federal Agencies, Homeland Defense

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
UNCLASSIFED	UNCLASSIFED	UNCLASSIFED	UNLIMITED	30	

USAWC STRATEGY RESEARCH PROJECT

ASSESSMENT OF U.S. CYBERSECURITY MANAGEMENT

by

Colonel Kelly T. Knitter
United States Army

Professor Brian Gouker
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Colonel Kelly T. Knitter

TITLE: Assessment of U.S. Cybersecurity Management

FORMAT: Strategy Research Project

DATE: 22 March 2012 WORD COUNT: 5,664 PAGES: 30

KEY TERMS: Cyber, Network Security, Information Technology, Information Sharing, Cyber Strategy, Cyber Stakeholders, Federal Agencies, Homeland Defense

CLASSIFICATION: Unclassified

In early 2009, President Obama declared cyber threat as one of the most serious economic and national security challenges of the 21st century. In May 2009, he directed the U.S. Government Accountability Office (GAO) to review national level cybersecurity policies and procedures. Findings indicated two critical shortfalls: lack of leadership and lack of clearly defined roles among federal agencies. Although a new Special Assistant to the President and Cybersecurity Coordinator was appointed within the White House three years ago to lead federal agencies in cyber collaboration and synchronization, the overall assessment given by GAO indicates cybersecurity management at the national level needs much improvement. The purpose of this paper is threefold: (1) to identify the different roles, responsibilities, and authorities of cybersecurity management within the U.S. Government; (2) to assess the national level cybersecurity management program for efficiencies and effectiveness; and (3) to provide strategic options on ways to improve overall cybersecurity management which leads to effective protection and operations of U.S. networks and information in a resource constrained environment.

ASSESSMENT OF U.S. CYBERSECURITY MANAGEMENT

> Cybersecurity threats represent one of the most serious national security, public safety, and economic challenges we face as a nation.
>
> —2010 National Security Strategy

Today's hackers are no longer thrill-seeking teenagers; they are organized crime syndicates, national militaries, and non-nation state organizations that commit espionage or have malicious intentions against people and infrastructure in order to compromise national security and/or economic interests. From thousands of miles away, increasingly sophisticated foreign adversaries are electronically infiltrating sensitive U.S. computer networks to obtain military technologies. In 2009, President Obama delivered a nation-wide informational speech to all American citizens saying, “Every day we see waves of cyber thieves trolling for sensitive information – the disgruntled employee on the inside, the lone hacker a thousand miles away, the industrial spy and, increasingly, foreign intelligence services.”[1] The intent of the speech was to alert the country that vital U.S. security interests are being attacked now, and in order to protect the populace, their assets, and America’s national interests, a robust U.S. cybersecurity strategic plan of action must be implemented immediately. The President went on to say, “It's the great irony of our Information Age -- the very technologies that empower us to create and to build also empower those who would disrupt and destroy.”[2] As the nation was transitioning from the Industrial Age to the Information Age, the President was cautioning the public that new technology intended to advance the world forward was having an opposite effect, and something must be done to change the tides.

To change the behavior and actions of the occasional hacker on up to the technologically advanced criminal mind, a new and creative strategic plan of action must be developed to alter the current path of destruction. The development of this plan must include participation from the U.S. Government, international communities, and private-public sectors alike to be effective, with a single point of authority providing guidance, direction and motivation to U.S. cybersecurity stakeholders. The purpose of this paper is to gain a better understanding of the cybersecurity management structure by assessing the current environment and key players, and then presenting options on how an improved national cybersecurity posture for the future can unfold with a proper plan of action. The intent of this paper is threefold: (1) to identify the different roles, responsibilities, and authorities of cybersecurity management within the U.S. Government; (2) to assess the national level cybersecurity management program for efficiencies and effectiveness; and then (3) to provide strategic options on ways to improve overall cybersecurity management which leads to effective protection and operation of U.S. networks and information in a resource constrained environment.

Background

In 2008, in response to ongoing threats to federal systems and operations posed by cyber attacks, President Bush directed the development of a new Comprehensive National Cybersecurity Initiative (CNCI). This initiative was designed to improve how the federal government protects sensitive information from hackers and nation states trying to break into agency and other networks. In addition, the decision to create the CNCI followed reports from multiple agencies having experienced a string of cyber attacks on their computer networks. The National Cyber Security Center (NCSC) was also established to coordinate information from federal agencies and departments to

secure networks and foster collaboration. The CNCI targeted reducing vulnerabilities, protecting against intrusions, and anticipating future threats, while the NCSC focused on formalizing existing cybersecurity processes and introducing new policies and business practices to better protect computer networks and systems.[3]

In early 2009, President Obama declared “cyber threat is one of the most serious economic and national security challenges the nation faces,” and that “America's economic prosperity in the 21st century will depend on cybersecurity.”[4] In May 2009, President Obama directed the U.S. Government Accountability Office (GAO) to review national level cybersecurity policies and procedures. The GAO results of the policy review focused specifically on cybersecurity responsibility. David Powner authored the GAO summary and indicated two critical shortfall findings: (1) lack of leadership and (2) lack of clearly defined roles among federal agencies. The lack of leadership concern began in March 2009 when the National Cyber Security Center director, Rod Beckstrom, quickly submitted his resignation letter to the Director of Department of Homeland Security (DHS) claiming lack of funding and prioritization of cybersecurity at the national level led to his decision to step down. As a result of Mr. Beckstrom’s resignation and the GAO’s assessment summary of the nation’s cybersecurity posture, a decision was made by the President to establish a Special Assistant to the President and Cybersecurity Coordinator within the White House to improve efficiencies in agency collaboration and synchronization. The new position would oversee cybersecurity management residing within the federal agency construct. To lead the nation’s cyber initiative, President Obama appointed Howard A. Schmidt, a former cybersecurity adviser to the White House under the Bush administration, and former head of

cybersecurity at Microsoft, as the nation's Cybersecurity Coordinator in December 2009.[5] The Coordinator has neither command authority nor budget authority over any federal agency, and the size of his administrative staff is extremely small to conquer the droves of cybersecurity issues plaguing the nation and the world in today's Information Age.

Much progress has been achieved within each respective federal agency towards cyber operations and policy development since December 2009, but a lack of a collective and cooperative effort among the different agencies still exists today. Even though a cybersecurity coordinator was appointed in the Executive Branch, the need for enhanced leadership and management in overseeing the nation's cybersecurity program is only now beginning to unfold. During periodic reviews of cybersecurity management conducted by the GAO, Federal agencies continue to report confusion when determining who has lead and support responsibilities on cybersecurity policies and initiatives. Because of role and responsibility uncertainties, duplication of effort and resourcing remain the same across the agencies causing unnecessary chaos and confusion.[6] One would think a duplication of efforts and resources would somehow increase and/or improve the productivity and the cybersecurity posture for the nation, since additional cybersecurity personnel and equipment are available to better accomplish the mission. However, greater progress is not being achieved due to lack of policies, leadership, bureaucracy, and information sharing. As each federal agency begins to develop similar policies, monitor and defend like networks, investigate criminal acts, coordinate with international and national private and public sectors, and perform identical research and development functions, it is obvious to the average observer (the

American citizen) that duplication of efforts is wasting away federal, state, and industry monies while the threat to national security is continuing to rise. As history books tell the story about the wild, wild West being fought and won, victory was achieved through proper leadership, structured and disciplined organizations, and clear strategy and vision. It was not won through adhoc committees, group consensus, and ambiguous direction through vague policies and wish lists. Therefore, the Federal Government needs to develop and execute a new cybersecurity strategy that takes into consideration lessons learned from the past, and anticipate requirements for the future. Developing "strategy on the move" and implementing Band-Aid solutions will only keep the country in a reactive cybersecurity posture. The world looks upon the United States as a leader in technology, development, and leadership. As cyber threats continue to spread across the globe at a rapid pace wreaking havoc on economic and security interests, the world needs a cyber role-model to effect change and make a positive difference. The United States needs to be out front and deliver this capability!

Roles and Responsibilities

Cybersecurity has been a focus within the United States Government since the 1980's, but taming the wild, wild West has been the problem.[7] To better understand the level of complexity within the cyber's "meshed" management arena, it is important to identify the key players within the U.S. Government who have a role in developing cybersecurity policies and operating procedures for the nation. In a recent article published by the Government Accountability Office in 2010, it identifies the following branches and federal agencies of having a significant role in cybersecurity: Executive Branch, Department of Homeland Security, Department of Defense, Department of Commerce, Department of Justice, and Department of State. This paper will focus on

the roles and responsibilities of these six federal agencies as they are the primary developers and implementers of cybersecurity policy and procedures.

Within the Executive Branch, the number one primary player is the new Cybersecurity Coordinator. This individual is a member of the National Security Staff and the Staff of the National Economic Council, with the responsibility of ensuring that federal cyber policies enhance the nation's security and embrace a coordinated approach across the government.[8] This individual is the pseudo Godfather of U.S. cybersecurity due to direct ties with the President, but lacks the money, the authority, and the control to influence people and processes across the cyber domain. Another department at the top of the Federal Government that has influence is the Office of Management and Budget, and its subordinate organization called the Office of E-Government and Information Technology (E-Gov). E-Gov is headed by the Federal Government's Chief Information Officer (CIO), and is responsible for developing and providing "direction in the use of Internet-based technologies to make it easier for citizens and businesses to interact with the Federal Government, save taxpayer dollars, and streamline citizen participation."[9] Mr. Steven VanRoekel is only the second Chief Information Officer of the United States, appointed by President Obama on August 5th, 2011. He succeded Mr. Vivek Kundra who served as the first CIO from March, 2009 to August, 2011 also under President Barack Obama. The CIO oversees the management of the CIO Council, which is the "principal interagency forum for improving agency practices related to the design, acquisition, development, modernization, use, sharing, and performance of Federal information resources."[10] The council includes members from 28 different federal executive agencies and a few other selected federal

organizations, and is one of many committee/councils established at the Executive Branch level to manage cybersecurity. Another important committee at the top is the Information and Communications Infrastructure Interagency Policy Committee (ICI-IPC), chaired by the National Security Council (NSC) and Homeland Security Council (HSC). The ICI-IPC is the primary information and communications infrastructure policy coordination body.[11]

Under Homeland Security Presidential Directive 23 and National Security Presidential Directive 54, the Department of Homeland Security (DHS) is officially the lead federal agency "defending federal executive branch networks and systems – the "dot-gov" domain – as well as coordination with the private sector to protect the nation's critical infrastructure and key resources."[12] DHS is primarily responsible for the defense of the federal information technology (IT) infrastructure and data networks. Most of the cybersecurity functions within this department are centralized under the Undersecretary of the National Protection & Programs Directorate.[13] One of the sub-directorates is the National Cyber Security Division (NCSD), which is tasked to "work collaboratively with public, private and international entities to secure cyberspace and America's cyber interest."[14] The NCSD Chief supervises the National Cybersecurity and Communications Integration Center (NCCIC) and the United States Computer Emergency Readiness Team (US-CERT). The NCCIC is a 24x7 center responsible for the production of a common operating picture for cyber and communications across the federal, state, and local governments; intelligence and law enforcement communities and the private sector."[15] The US-CERT is also a 24x7 center, and the operational arm of the NCSD. It is charged with providing response support and defense against cyber

attacks for the Federal Civil Executive Branch (.gov) and information sharing and collaboration with state and local governments, industry and international partners.[16] DHS/NCSD leads a number of programs to protect cyber infrastructure from attack, such as the National Cyber Response Coordination Group. This group is comprised of thirteen federal agencies, and is responsible for coordinating a synchronized federal response in the event a nationally significant cyber event occurs.[17] Another directorate within DHS who has a prominent role in cybersecurity is the U.S. Secret Service (USSS). On October 26, 2001, President Bush signed into law the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act,"[18] which directed the USSS to establish a nationwide network of Electronic Crimes Task Forces (ECTFs). The ECTF network brings together not only federal, state and local law enforcement, but also prosecutors, private industry and academia.[19] The task forces are one of many units responsible for investigating cybercrimes within the nation's borders. The USSS mission is to safeguard the nation's financial infrastructure and payment systems to preserve the integrity of the economy,[20] by reducing "the amount of financial losses resulting from electronic crimes, financial crimes, computer crimes, compromised payment systems, identity theft and other types of financial crimes."[21] And finally, the last key cyber player to recognize within DHS is the Information Sharing and Analysis Center (ISAC). This initiative was created to build partnerships between DHS and external organizations to the federal government. In 2003, the Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection (HSPD-7)[22] was signed, in which the "Federal Government asked each critical infrastructure sector to establish

sector specific information sharing organizations to share information, within each sector, about threats and vulnerabilities to that sector."[23] In response, many sectors created an ISAC to meet the demands addressed within HSPD-7. Currently, there are sixteen ISAC teams developed, and they meet quarterly: Electric Sector, Financial Services, Information Technology, Surface Transportation, Public Transit, Communications, Water, Multi-State, Real Estate, Research and Education, Supply Chain, Nuclear, Maritime, Highway, National Health, and Emergency Management and Response.[24] All partnerships have written agreements which allow non-federal members to work within the 24x7 cyber operations cell within the NCCIC on a daily basis, when participating in joint cyber exercises, and when responding to real-world cyber crises. The collaboration and synchronization between both federal and non-federal cyber professionals has been instrumental in protecting America's infrastructure and information networks.

The Department of Defense (DoD) – offensive and defensive cyber operations - is closely partnered with DHS – defensive cyber operations - to ensure the full spectrum of operations (defense, exploit, and attack) is well achieved and synchronized to safeguard the nation from a cyber threat. A formal Memorandum of Agreement was signed in September 2010 by both leaders of DHS and DoD to increase interdepartmental collaboration, to improve cooperation, and to better define roles and responsibilities in order to prevent duplication of effort.[25] In 2010, the DoD created a new command headquarters, U.S. Cyber Command (USCYBERCOM), which is a sub-unified command under the U.S. Strategic Command. Its mission is to plan, coordinate, integrate, synchronize, and direct activities to operate and defend the Department of

Defense information .mil networks and, when directed, conduct full-spectrum military cyberspace operations in order to ensure U.S. and allied freedom of action in cyberspace, while denying the same to our adversaries.[26] The subordinate operating arms of USCYBERCOM represent each military service into the fold: the Army Forces Cyber Command (ARCYBER), the Navy's Fleet Cyber Command (FLTCYBERCOM), the Twenty-Fourth Air Force (AFCYBER), and the Marine Forces Cyber Command (MARFORCYBER). In addition to each military service contribution, the Commander of USCYBERCOM is also dual-hatted as the Director of the National Security Agency (NSA) and the Chief of the Central Security Service (CSS). The NSA/CSS leads the U.S. cryptologic community on the signals intelligence and information assurance fronts. This increased partnership and collaboration initiative linked the nation's cyber intelligence arm with the cyber arm for military cyber management. The three lines of operations within USCYBERCOM are: DoD Global Information Grid operations (management of IT networks); [27] defensive cyberspace operations (preventing cyber attacks);[28] and offensive cyberspace operations (performing cyber exploits and attacks).[29] Again, DoD has the lead role in cyber exploitation and cyber attack operations.

The Department of Commerce (DoC) is another major player within the national cybersecurity framework that is responsible for improving technology for cyber systems and developing critical IT infrastructure design templates for federal networks. The DoC cyber authority is captured in the Defense Production Act of 1950, which allows for contracting and spending provisions by federal agencies to meet national defense requirements.[30] DoC has two important organizations that pertain to security of

computer networks, the National Institute of Standards and Technology (NIST) and the National Telecommunications and Information Administration (NTIA). The NIST is the Research, Development, Technology, and Engineering (RDT&E) arm for DoC. It is responsible for developing, testing, disseminating, monitoring, and measuring new information technology (IT) principles and mechanics underlying security standards, metrics, and best practices for commercial and governmental entities.[31] The NTIA is the agency providing direct support to the Executive Branch, and is principally responsible for advising the President on telecommunications and information policy issues. Its programs and policymaking focus largely on expanding broadband Internet access and adoption in America. NTIA develops policies on issues related to the Internet economy, including online privacy, cybersecurity, and the global free flow of information online.[32]

The Department of Justice (DoJ) is the chief law enforcement agency of the U.S. Government and is responsible for developing cyber rules of engagement and laws established by Congress, and prosecuting individuals, businesses, agencies, States and Nations who violate cyber-related laws.[33] A subordinate agency is the Federal Bureau of Investigations (FBI), who leads the national efforts in investigating and prosecuting cybercrimes.[34] The cybersecurity mission of the FBI is investigating high-tech crimes, such as cyber-based terrorism, computer intrusions, online sexual exploitation, and major cyber frauds.[35] The FBI gathers information from public and private sectors, commercial businesses, and other federal agencies in order to analyze the forensic evidence of a cybercrime scene to identify the origin or author of the malicious activity. The FBI partners with other law enforcement agencies (federal, state, municipal, and international agencies) to protect and defend the nation against

terrorist and foreign intelligence threats, and to uphold and enforce U.S. criminal laws.[36] The National Cyber Investigative Joint Task Force (NCIJTF) is overseen by the FBI, and includes representation from the U.S. Secret Service and several other federal agencies. This cyber investigation coordination organization serves as a multi-agency national focal point for coordinating, integrating and sharing pertinent information related to cyber threat investigations.

The Department of State (DoS) is the lead agency responsible for foreign affairs, and therefore, has a significant role in formulating, coordinating, and overseeing the implementation of international communications and information policy. Under the 2003 National Strategy to Secure Cyberspace, the DoS was charged with leading federal efforts to enhance international cyberspace security cooperation.[37] To fill the department's lead responsibility, a number of directorates are given a role. For example, the Bureau of Economic, Energy, and Business Affairs, International Communications and Information Policy (EEB/CIP) is accountable for international telecommunications and information policy. In addition, the Bureau of Intelligence and Research (INR), Office of Cyber Affairs provides intelligence analysis and coordinates international outreach on cybersecurity issues.[38]

As cybersecurity roles and responsibilities continue to mature among the different federal agencies, it is apparent that redundant and duplicative efforts in cyber defense operations, policy development, law enforcement, and research and development initiatives exist within multiple agencies of the U.S. Government. A key reason for such cyber duplicity is the lack of an appointed single authority representative responsible for overall cybersecurity management. Where is the leader

required to supervise unity of command and unity of effort, and to manage financial requirements and human resources within an organization? It is non-existent within the limits of the U.S. Government. An indicator of chaos within the realm of cybersecurity management is clearly noticeable with the resignation of senior cyber officials over the past few years. These senior federal leaders are stepping away from the chaos of disorganization and mis-management, ultimately impeding progress in managing the cyber domain.

Assessment of Cybersecurity Management

As the cyber domain continues to grow in size and power every day, the number of follow-on cyber threats and vulnerabilities also increases exponentially. Due to increasing security threats on national interests and infrastructure, time is of the essence to ensure the nation has a responsive and effective cybersecurity management structure capable of addressing the global aspects of cyberspace. "The U.S. government faces a number of challenges that impede its ability to formulate and implement a coherent approach"[39] to global cyberspace, including (1) providing top-level leadership, (2) developing a coherent and comprehensive strategy, (3) coordinating across all relevant federal entities, (4) ensuring cyberspace-related technical standards and policies do not pose unnecessary barriers to U.S. trade, (5) participating in international cyber incident response, (6) differing legal systems and enforcing U.S. criminal and civil laws, and (7) defining international norms for cyberspace.[40] To address the challenges identified, the Special Assistant to the President and Cybersecurity Coordinator, in collaboration with other federal entities and the private sector, must create a united front to establish cyber capabilities consistent with our national economic and national security interests.[41]

Concurring with the Government Accountability Office's assessment in 2010, the Federal government is definitely not structured to address the growing problem of cybersecurity effectively now or in the future. Roles and responsibilities for cybersecurity are dispersed across a wide array of federal departments and agencies, many with overlapping authorities, and none with sufficient decision making authority to direct actions that deal with often conflicting issues in a consistent way. The strategic vision and plan the government needs to integrate must be holistic to meet the demands of cybersecurity-related issues confronting the U.S. Government. The Nation needs to develop the policies, processes, people, and technology required to mitigate cybersecurity-related risks.[42]

Max Stier stated, "Time is overdue for the government to commit the resources and exert the leadership to build and nurture a highly skilled cyber workforce" that is properly structured, carefully concerned about citizen and national interests, and globally focused to thwart cyber threats and vulnerabilities.[43] In the article, *The Cybersecurity Triad: Government, Private Sector Partners, and the Engaged Cybersecurity Citizen,* the authors Harknett and Stever argue the "need for an engaged and knowledgeable public on cybersecurity must be equal to a well-structured and managed government."[44] They highlight the importance of maintaining a proper balance of commitment between the U.S. Government and the citizens, because without the engagement of each citizen becoming a cybersecurity provider, the national objective of having a secure cyberspace will never be achieved. To achieve success, the government must partner with the populace to become individual IT protectors, not just

beneficiaries of security policies.[45] The unanswered question is, “Which federal agency is responsible?”

According to the 2011 National Strategy to Secure Cyberspace, the U.S. Government recognized that securing cyberspace is a global matter due to the interconnectedness of the world’s computer systems, and that a global solution is necessary to safeguard information and protect against infrastructure and economic threats. Incorporating international cooperation and collaboration efforts to mitigate cyber threats demands open communication and a lot of trust. Great strides have occurred over the past few years by cyber engineers, incident responders, policy developers, intelligence analysts, and law enforcers to recognize the importance of sharing cybersecurity information across international boundaries, and incorporating global solutions into cross-border security problem sets. The greater problem lies with the accuracy and wholeness of data, and the expediency of the information gathering and sharing processes. With the current multi-agency cyber construct and duplication of cyber efforts within the U.S. Government, it is a monumental task for the American citizen and business owner to determine which federal agency to call for support; and an even more difficult task for the international cyber community to leverage the U.S. for support. Albeit pre-coordinated formal agreements, policies, and treaties reduce the information sharing time lapse, but new threat tactics, techniques, and procedures entering into the world networks often require new response actions and new coordination partners; making already approved agreements outdated and obsolete.

As it is well known, yesterday’s sophisticated hacker utilizing zero-day exploits[46] to slow or stop networks is no match with tomorrow’s advanced persistent threat (APT),

which are state and non-state crime organizations that exfiltrate intellectual property to support their criminal activities. The international community requires safe and assured networks where critical information is able to traverse boundary lines freely, and reliance on protecting infrastructure is amplified as a global interest, and not only a national interest. In order to stay one step ahead of the ever-increasing global cyber threat, U.S. international partners should have a centralized location, a one-stop-shop, to collaborate cybersecurity issues. The unanswered question is, "Which federal agency is responsible?"

Securing global cyberspace requires individual, public, private, local, state, federal, and international cooperation to raise awareness, share information, promote security standards, and investigate and prosecute cybercrime.[47] In order to reach this plateau of properly managed cybersecurity measures, it is necessary, not only for the United States, but for the world as a whole, that a unified effort of command is established in America that will promote overall stability and security.

Strategic Options Improving Cybersecurity Management

After reviewing the roles and responsibilities within each federal agency, and the assessment of current cybersecurity management, the author proposes three options for consideration in addressing the global aspects of cyberspace and improving cyber management within the national boundaries: (1) maintain status quo organizational structure, (2) realign organizational structure, and (3) create a new cyber agency. The information below highlights the advantages, disadvantages and strategic consequences of each option.

OPTION I (Maintain the Status Quo). This option requires no change to current organizational structures within the National Security Staff and Federal Agencies. Since

the Special Assistant to the President and Cybersecurity Coordinator is relatively a new position established in Dec 2009, the cyber program is still in its infancy stage in managing cybersecurity activities and has yet to mature into a robust management element. The option of maintaining status quo would improve overall management of the cyber domain through time and on-the-job experience. The most significant advantage of this option is the no-cost payload. The financial requirement to "stay the course" and mature the Coordinator's position over time best meets today's economic demands for reduced governmental spending as this option incurs no financial obligations for restructuring. The disadvantages are: insufficient manpower to workload demands; unresolved prioritization of tasks and defining roles and responsibilities; and untimely management of cyber security operations and policy development. The potential strategic consequences are three-fold: (1) increased network attacks and delayed cyber incident response actions due to lack of policies and synchronized exchange of information; (2) decreased cyber collaboration within the international community due to limited management oversight; and (3) increased recovery costs to restore attacked infrastructure. All concerns place significant risks to national security interests, diplomatic measures and economic initiatives.

OPTION II (Realign the Organizational Structure). This option consists of the establishment of an executive level "cyber council" with membership representing cyber stakeholders from each Federal Agency, and assigning them under the Cybersecurity Coordinator office for command and control. The assumption is the new panel of twenty-plus members would create an immediate organizational staff to off-set the heavy workload of the Cybersecurity Coordinator. Developing a productive and skilled

staff would be advantageous to both the Executive Branch and Federal Agencies as timely and improved interagency communications will begin to take hold. Acceptance does require federal agency buy-in on developing a new organizational structure. Other advantages include: prioritization of effort, delineation of responsibilities, balanced distribution of workload, and improved collaboration across international borders. The international advantage would be achieved through cyber council member participation in global information exchanges on policies and procedures, and incident response actions on cyber attacks. The disadvantage is a higher cost than maintaining the status quo organizational structure. Cost is minimized due to office space allocation and relocation of personnel. The strategic consequences of implementing this option are significantly reduced compared to options I and III. All national elements of power (diplomatic, information, military, and economic) are successfully incorporated through the strengthening of global partnerships, enabling of governance and organizational structure, dissuading and deterring the cyber threat, and prevention of further economic hardships. Realigning personnel from other federal agencies in a timely manner is absolutely feasible. Although very positive in improving leadership and coordination, this option does not resolve the lack of budgetary authority over cybersecurity management.

OPTION III (Create a New Cyber Agency). This option establishes a new Federal Agency responsible for leading all cyber-related activities, including the development and implementation of policies and procedures; information sharing and synchronization of cyber operations at the local, state, federal, and international coordination levels; monitoring the cyber domain for intrusions; conducting forensic

analysis; coordinating intelligence and law enforcement initiatives; performing RDT&E; and developing comprehensive strategy. The Cyber Coordinator would remain as an appointee on the Presidential Staff to alert the President and Executive Branch members of national level cyber updates, and be a liaison between the White House and the new cyber headquarters.

In an attempt to reduce the duplication of effort and resources currently straining the management process, a detailed assessment of all federal agencies would be conducted to identify the cyber elements for potential reorganization. This would require an external agency of the federal government to lead this assessment team with additional members consisting of representatives from each federal department and agency. Establishing the new headquarters workforce would either come from other existing Federal Agency billets, or a combination of new and transferred employees. The latter option of developing a blended workforce with new and current Federal employees is the preferred solution in order to prevent total disruption in long-established agencies and to create new jobs. Elements for possible consolidation are policy writers, research and development scientists, federal network operation centers, and intelligence analysts. Creating a new agency would not eliminate the need for interagency communication and collaboration; in fact, the need would be greater. Today's governmental environment is, and will always be, a meshed network of systems and power. The management of intelligence, economics, military, law enforcement, and foreign affairs are not only governed by separate federal agencies, but each element is also a sub-set of every federal agency. For example, each department currently has an international security cooperation requirement, a budget

division, a law and policy section, and a cyber-threat analysis cell; the same can be said with communications and information management. Although cyber is a common factor among all federal agencies, the future of cyber operations will continue to grow exponentially in the public, private, and federal sectors. The world has only seen the beginning of technology, to include cyber attacks and cybersecurity. If the majority of America's networks are located in the private sector, then most cybersecurity risk is located in this environment, and it is mainly economic. It is the remainder of America's networks, such as: .gov and .mil, that have the heavy load of sensitive or classified information, and subsequently are already the best protected. The disadvantage to this option is the cost in creating a new headquarters.

Recommendation

As today's criminals and terrorists continue to penetrate the global information grid, the need to protect vital U.S. security interests is critical. However, time is of essence in order to achieve measurably improved unity of effort in managing the cyberspace. The best option to consider in the near term which will guarantee immediate results and minimal use of resources is Option II, realignment of the current cybersecurity organizational structure. This plan meets the objectives for better leadership, improved global and interagency collaboration, timely development and enforcement of policies and procedures, increased oversight of cyber operations, enhanced national security posture, and reduced economic spending. The key to success is a well-established management structure with authoritative powers to guide, direct and motivate the cybersecurity workforce. Option II is the best solution to resolve current shortfalls in today's cybersecurity management structure.

The long term solution, however, remains with Option III, create a new cyber agency. Establishing a new headquarters would not only improve cyber management within the nation, it would show the international community the U.S. takes cybersecurity as a national priority, and could create a sense of cyber dominance over other nation-state or non-nation-state adversaries. Other advantages to this option are centralized authority, centralized decision making, minimized duplication of effort, and clear lines of roles and responsibilities. Although an operational needs statement can be written to justify a new cybersecurity federal agency based solely on the threat, the amount of time and resources needed to get congressional approval and establish an effective and efficient organization are without a doubt a difficult and complex task to accomplish. The financial burden alone would counter today's economic plan for reduced spending, and potentially cause unrest within the public sector; even though new jobs could be created. A comprehensive strategy road map and robust strategic communications plan would be required to gain approval from Congress and the public at large to move forward with this option.

Conclusion

Our Nation's senior policymakers must think through the long-range strategic options available to the United States in a world that depends on assuring the use of cyberspace. To date, the U.S. Government has been implementing traditional approaches to the cybersecurity problem—and these measures have not achieved the level of security needed. The 2008 CNCI and its follow-on efforts are aimed at building an approach to cyber defense strategy that deters interference and attack in cyberspace by improving warning capabilities, articulating roles for private sector and international partners, and developing appropriate responses for both state and non-state actors.

New, non-traditional approaches to cybersecurity are needed to breach the ineffective "rice bowl" protectionism of current cybersecurity organizations. Shared intelligence between the government and private sector cybersecurity operations centers would be a first, important step. Merging the Federal cybersecurity organizations and capabilities, to the extent that duplication of effort and operations are measurably reduced, is a second step that might lead to cost savings while improving our nation's cybersecurity posture. Growing cyber-savvy leadership, perhaps from the ranks of the technologically brilliant private and federal sectors, to replace the folks that do not "get it", but are in positions of authority is a third step. The challenge is to change the culture of how we solve the Nation's cybersecurity issues in harmony with the tremendous assets at our disposal to do so.

Endnotes

[1] President Barack A. Obama, Speech: Securing our Nation's Cyber Infrastructure, May 29, 2009, http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure (accessed October 18, 2011).

[2] Ibid.

[3] David A. Powner, "Summary Cybersecurity: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative," *Government Accountability Office*, no. GAO-10-338 (March 5, 2010): 1.

[4] President Barack A. Obama, Speech: Securing our Nation's Cyber Infrastructure, May 29, 2009, http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure (accessed October 18, 2011).

[5] David A. Powner, "Summary Cyberspace Policy: Executive Branch Is Making Progress Implementing 2009 Policy Review Recommendations, but Sustained Leadership Is Needed," *Government Accountability Office*, no. GAO-11-24 (October 6, 2010): 1.

[6] Ibid.,4.

[7] James A. Lewis and Katrina Timlin, "Cybersecurity and Cyberwarfare*," UNIDIR Resources,* 2011*,* http://www.unidir.org/pdf/ouvrages/pdf-1-92-9045-011-J-en.pdf (accessed December 18, 2011).

[8] President Barack A. Obama, Speech: Securing our Nation's Cyber Infrastructure, May 29, 2009, http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure (accessed October 18, 2011).

[9] The *Office of Management and Budget, E-Gov Home Page*, http://www.whitehouse.gov/omb/egov (accessed December 7, 2011).

[10] The *Office of Management and Budget, CIO.gov Home Page*, http://www.cio.gov/council-about.cfm/csec/1 (accessed January 12, 2012).

[11] Cyberspace Policy Review, "Assuring a Trusted and Resilient Information and Communications Infrastructure," *2011,* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf, (accessed January 12, 2012).

[12] The *Department of Homeland Security, Cybersecurity Home Page*, http://journal.dhs.gov/2009/06/focused-effort-on-cybersecurity.html (accessed February 8, 2012).

[13] James A. Lewis and Katrina Timlin, "Cybersecurity and Cyberwarfare*," UNIDIR Resources,* 2011*,* http://www.unidir.org/pdf/ouvrages/pdf-1-92-9045-011-J-en.pdf (accessed December 18, 2011).

[14] The *Department of Homeland Security, National Cyber Security Division Home Page*, <www.dhs.gov/xabout/structure/editorial_0839.shtm> (accessed February 27, 2012).

[15] The *Department of Homeland Security, National Cybersecurity and Communications Integration Center (NCCIC) Home Page*, http://www.dhs.gov/files/programs/nccic.shtm (accessed February 27, 2012).

[16] The *Department of Homeland Security, United States Computer Emergency Readiness Team (US-CERT) Home Page*, http://www.us-cert.gov/aboutus.html (accessed December 7, 2011).

[17] The White House, "Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection," December 17, 2003, http://www.fas.org/irp/offdocs/nspd/hspd-7.html (accessed November 8, 2011).

[18] The *United States Department of the Treasury, Financial Crimes Enforcement Network Home Page*, http://www.fincen.gov/statutes_regs/patriot/ (accessed November 8, 2011).

[19] The *Department of Homeland Security, U.S. Secret Service Website, Electronic Crimes Task Forces and Working Groups Home Page*, http://www.secretservice.gov/mission.shtml (accessed November 29, 2011).

[20] Ibid.

[21] Ibid.

[22] The White House, "Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection," December 17, 2003, http://www.fas.org/irp/offdocs/nspd/hspd-7.html (accessed November 8, 2011).

[23] National Council of ISACs, "The Role of Information Sharing and Analysis Centers (ISACS) in Private/Public Sector Critical Infrastructure Protection," January 2009, 4, http://www.isaccouncil.org/ (accessed December 20, 2011).

[24] The *National Council of ISACs Home Page*, http://www.isaccouncil.org/ (accessed March 18, 2012).

[25] Memorandum of Agreement between DHS and DoD Regarding Cybersecurity, September 2010, http://www.dhs.gov/xlibrary/assets/20101013-dod-dhs-cyber-moa.pdf (accessed March 20, 2012).

[26] The *United States Strategic Command, U.S. CYBERCOM Home Page*, http://www.stratcom.mil/factsheets/cyber_command/ (accessed February 2, 2012).

[27] DOD Global Information Grid operations are actions taken to direct, and provide guidance and unity of effort to support efforts to design, build, configure, secure, operate, maintain, and sustain DOD networks to create and preserve availability, integrity, authentication, confidentiality and non-repudiation of information. Proactive Network Operations, the major operational method by which U.S. Cyber Command will conduct this line of operation, anticipates vulnerabilities and takes actions to preserve availability, confidentiality, integrity, and non-repudiation prior to the discovery of threats and intrusions. U.S. Cyber Command, *USCYBERCOM Concept of Operations*, Version 1.0 (October 22, 2011).

[28] Defensive cyberspace operations direct and synchronize actions to detect, analyze,counter, and mitigate cyber threats and vulnerabilities; to outmaneuver adversaries taking or about to take offensive actions; and to otherwise protect critical missions that enable U.S. freedom of action in cyberspace. This line of operation can trigger offensive cyberspace operations or other response actions necessary to defend DOD networks in response to hostile acts, or demonstrated hostile intent. Dynamic Network Defense Operations, the key U.S. Cyber Command operational method for defensive cyberspace operations, are those machine-synchronized and other actions to rapidly detect, analyze, counter and mitigate threats and vulnerabilities to DOD information networks. This line of operation is informed by timely intelligence, threat indicators, vulnerability information, and effects assessment information from the other lines of operation. U.S. Cyber Command, *USCYBERCOM Concept of Operations*, Version 1.0 (October 22, 2011).

[29] Offensive cyberspace operations are the creation of various enabling and attack effects in cyberspace, to meet or support national and combatant commander's objectives and to actively defend DOD or other information networks, as directed. The primary U.S. Cyber Command offensive operational method will be effects-based operational planning and execution, maximizing leveraging and coordination across DOD and the interagency to meet objectives. Offensive targeting will be conducted using the guidance, apportionment, and tasking process. U.S. Cyber Command, *USCYBERCOM Concept of Operations*, Version 1.0 (October 22, 2011).

[30] David A. Powner, "Cyberspace – U.S. Faces Challenges in Addressing Global Cybersecurity and Governance," *Government Accountability Office*, no. GAO-10-606 (July 2010): 18.

[31] The *Department of Commerce, National Institute of Standards and Technology Home Page,* http://www.nist.gov/index.html (accessed March 1, 2012).

[32] The *Department of Commerce, National Telecommunications and Information Administration Home Page*, http://www.ntia.doc.gov/ (accessed March 1, 2012)

[33] David A. Powner, "Cyberspace – U.S. Faces Challenges in Addressing Global Cybersecurity and Governance," *Government Accountability Office*, no. GAO-10-606 (July 2010): 23.

[34] The White House, "National Strategy to Secure Cyberspace," 2003, http://georgewbush-whitehouse.archives.gov/pcipb/ (accessed March 20, 2012).

[35] The *Federal Bureau of Investigations, Cyber Crime Home Page*, http://www.fbi.gov/about-us/investigate/cyber (accessed February 3, 2012).

[36] The *Federal Bureau of Investigations, Cyber Crime Home Page*, http://www.fbi.gov/about-us/investigate/cyber/addressing-threats-to-the-nations-cybersecurity (accessed February 3, 2012).

[37] David A. Powner, "Cyberspace – U.S. Faces Challenges in Addressing Global Cybersecurity and Governance," *Government Accountability Office*, no. GAO-10-606 (July 2010): 26.

[38] Ibid.

[39] David A. Powner, "Cyberspace – U.S. Faces Challenges in Addressing Global Cybersecurity and Governance," *Government Accountability Office*, no. GAO-10-606 (July 2010): 30.

[40] Ibid.

[41] Ibid., 26.

[42] Cyberspace Policy Review, "Assuring a Trusted and Resilient Information and Communications Infrastructure," http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf, 2011 (accessed January 15, 2012).

[43] Max Stier, "Government Should Help Widen Cyber Knowledge*,"* http://www.federaltimes.com/article/20090914/ADOP06/909140302/1037/ADOP00 (accessed November 20, 2011).

[44] Richard Harknett and James Stever, "The Cybersecurity Triad: Government, Private Sector Partners, and the Engaged Cybersecurity Citizen," July 6, 2010, http://www.nsci-va.net/WhitePapers/2010-07-06-Cyber%20Training%20and%20Education%20Whitepaper-Crouch-McKee-final.pdf (accessed March 20, 2012).

[45] Ibid.

[46] A zero-day exploit is a no-notice launch of an offensive computer code by an adversary that is unprotected by current network defense procedures. These exploits significantly increase the risk levels of protecting and safeguarding information and infrastructure.

[47] Davi M. D'Agostino, "Defense Department Cyber Efforts, More Detailed Guidance Needed to Ensure Military Services Develop Appropriate Cyberspace Capabilities," *Government Accountability Office*, no. GAO-11-421, May 2011, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (accessed February 8, 2012).